BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－51439

(43)公開日　平成10年(1998)２月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ａ
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ａ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ａ
	9/32					６０１Ｃ
						６０１Ｅ

審査請求　未請求　請求項の数22　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願平9－129972

(22)出願日　平成９年(1997)５月20日

(31)優先権主張番号　特願平8－126751

(32)優先日　平８(1996)５月22日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

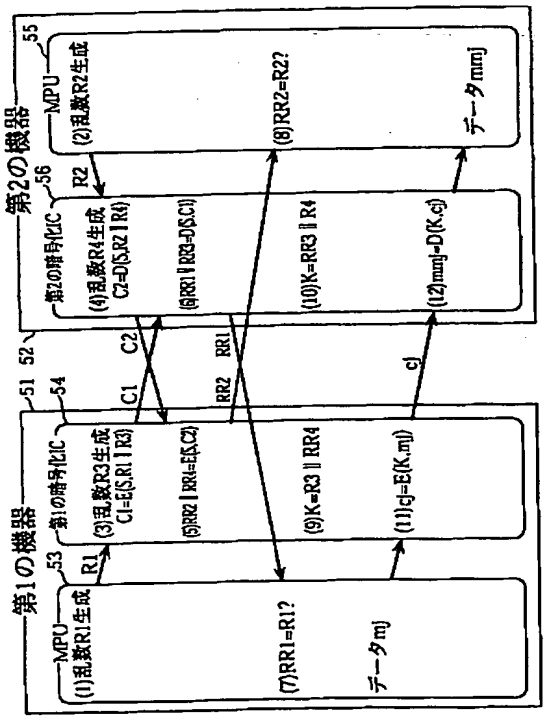
(74)代理人　弁理士　中島　司朗

(54)【発明の名称】　暗号化装置

(57)【要約】

【課題】　規模の小さな暗号化ＩＣを備え、機器間通信の安全性を確保するための必要最小限の機能を有する暗号化装置を提供する。

【解決手段】　第１の機器５１において、第１の暗号化ＩＣ５４は、第２の機器を認証する過程（ステップ(1)、(3)、(6),(7)）で生成した乱数Ｒ３と、自らの正当性を第２の機器５２に対して証明する過程（ステップ(2)、(4)、(5),(8)）で獲得した乱数ＲＲ４とを結合することで時変のデータ転送鍵を生成し（ステップ(9)）、そのデータ転送鍵を用いてデジタル著作物を暗号化し、第２の機器５２に転送する（ステップ(11)）。



1

【特許請求の範囲】

【請求項１】　データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、

前記データ転送鍵の共有化のための第１乱数を生成する第１乱数生成手段と、

前記第１乱数生成手段により生成された第１乱数を保持する第１乱数保持手段と、

前記第１乱数生成手段により生成された第１乱数を前記暗号通信の相手機器に送信する第１送信手段と、

前記第１乱数保持手段に保持された第１乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、

暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、

前記第１乱数生成手段、前記第１乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、１個のＩＣ内の回路で実現され、

前記第１乱数保持手段は、前記ＩＣの外部からアクセスできない領域に前記第１乱数を保持することを特徴とする暗号化装置。

【請求項２】　前記暗号化装置はさらに、前記第１乱数生成手段により生成された第１乱数を暗号化する第１暗号化手段を備え、

前記第１暗号化手段は、前記ＩＣ内の回路で実現され、

前記第１送信手段は、前記第１暗号化手段で暗号化された第１乱数を前記相手機器に送信することを特徴とする請求項１記載の暗号化装置。

【請求項３】　前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、

前記暗号化装置はさらに、

前記相手機器に送信するチャレンジデータ用の第２乱数を生成する第２乱数生成手段と、

前記チャレンジデータに対して前記相手機器から返信されてきたレスポンスデータと前記第２乱数とが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段とを備え、

前記データ転送鍵生成手段は、前記認証がなされた場合に前記データ転送鍵を生成することを特徴とする請求項２記載の暗号化装置。

【請求項４】　前記第２乱数生成手段及び前記認証手段は、前記ＩＣ外の回路で実現されていることを特徴とする請求項３記載の暗号化装置。

【請求項５】　前記暗号化装置はさらに、

前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、

復号化された結合データをレスポンスデータに相当する第１分離データと残る第２分離データとに分離する分離手段と、

前記第１分離データを前記相手機器に返信する第２送信手段とを備え、

前記第１暗号化手段は、前記第１乱数と前記第２乱数とを結合し、その結果得られた結合データを暗号化し、

前記データ転送鍵生成手段は、前記第１乱数と前記第２分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段及び前記分離手段は、前記ＩＣ内の回路で実現されていることを特徴とする請求項４記載の暗号化装置。

【請求項６】　前記暗号化装置はさらに、

前記第２乱数をチャレンジデータとして前記相手機器に送信する第２送信手段と、

前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、

復号化された結合データをレスポンスデータに相当する第１分離データと残る第２分離データとに分離する分離手段とを備え、

前記認証手段は、前記第１分離データを前記相手機器から返信されてきたレスポンスデータとして前記判断及び認証をし、

前記第１暗号化手段は、前記相手機器から送信されてきたチャレンジデータと前記第１乱数とを結合し、その結果得られた結合データを暗号化し、

前記データ転送鍵生成手段は、前記第１乱数と前記第２分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段及び前記分離手段は、前記ＩＣ内の回路で実現されていることを特徴とする請求項４記載の暗号化装置。

【請求項７】　前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第１暗号化手段及び前記復号化手段の少なくとも１つのものと同一であることを特徴とする請求項５又は６記載の暗号化装置。

【請求項８】　前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第１暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であることを特徴とする請求項５又は６記載の暗号化装置。

【請求項９】　前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化することを特徴とする請求項８記載の暗号化装置。

【請求項１０】　前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうことを特徴とする請求項９記載の暗号化装置。

【請求項１１】　前記第１暗号化手段での暗号と前記復号化手段での復号化とは、同一の変換アルゴリズムであ

ることを特徴とする請求項１０記載の暗号化装置。

【請求項１２】　前記第１暗号化手段及び前記復号化手段は、予め前記ＩＣ内に保持された鍵データを用いて前記暗号化及び復号化を行い、

その鍵データの一部は、前記ＩＣ内のマスクＲＯＭ領域に格納され、残る一部は、前記ＩＣ内の追記ＲＯＭ領域に格納されていることを特徴とする請求項１１記載の暗号化装置。

【請求項１３】　前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、

前記暗号化装置はさらに、

前記チャレンジデータに対して前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、

復号化された結合データをレスポンスデータに相当する第１分離データと残る第２分離データとに分離する分離手段と、

前記第１乱数と前記第１分離データとが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段と、

前記認証がなされた場合に前記第２分離データを暗号化する第２暗号化手段と、

暗号化された前記第２分離データをレスポンスデータとして前記相手機器に返信する第２送信手段とを備え、

前記データ転送鍵生成手段は、前記第１乱数と前記第２分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段、前記分離手段及び前記第２暗号化手段は、前記ＩＣ内の回路で実現されていることを特徴とする請求項２記載の暗号化装置。

【請求項１４】　前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第１暗号化手段、前記第２暗号化手段及び前記復号化手段の少なくとも１つのものと同一であることを特徴とする請求項１３記載の暗号化装置。

【請求項１５】　前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第１暗号化手段、前記第２暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であることを特徴とする請求項１３記載の暗号化装置。

【請求項１６】　前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化することを特徴とする請求項１５記載の暗号化装置。

【請求項１７】　前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうことを特徴とする請求項１６記載の暗号化装置。

【請求項１８】　前記第１暗号化手段及び前記第２暗号化手段での暗号化と前記復号化手段での復号化とは、いずれも同一の変換アルゴリズムであることを特徴とする請求項１７記載の暗号化装置。

【請求項１９】　前記第１暗号化手段、前記第２暗号化手段及び前記復号化手段は、予め前記ＩＣ内に保持された鍵データを用いて前記暗号化及び復号化を行い、

その鍵データの一部は、前記ＩＣ内のマスクＲＯＭ領域に格納され、残る一部は、前記ＩＣ内の追記ＲＯＭ領域に格納されていることを特徴とする請求項１８記載の暗号化装置。

【請求項２０】　データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、

それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞれ、

チャレンジデータ用の第１乱数を生成する第１乱数生成手段と、

前記データ転送鍵用の第２乱数を生成する第２乱数生成手段と、

前記第１乱数と前記第２乱数を結合する結合手段と、

前記結合データを暗号化する暗号化手段と、

暗号化された前記結合データを前記相手機器に送信する第１送信手段と、

前記相手機器の第１送信手段から送信された暗号化された結合データを受信する第１受信手段と、

受信した前記結合データを復号化する復号化手段と、

復号化された前記結合データをレスポンスデータに相当する第１分離データと前記データ転送鍵用の第２分離データに分離する分離手段と、

前記第１分離データをレスポンスデータとして前記相手機器に返信する第２送信手段と、

前記相手機器の第２送信手段から返信された第１分離データを受信する第２受信手段と、

受信した前記第１分離データと前記第１乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、

前記第２乱数と前記第２分離データとを結合することで、前記データ転送鍵を生成するデータ転送鍵生成手段と、

前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする暗号化装置。

【請求項２１】　データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、

それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞ

れ、
チャレンジデータ用の第１乱数を生成する第１乱数生成手段と、
前記第１乱数を前記相手機器に送信する第１送信手段と、
前記相手機器の第１送信手段から送信された第１乱数を受信する第１受信手段と、
前記データ転送鍵用の第２乱数を生成する第２乱数生成手段と、
受信した前記第１乱数と前記第２乱数を結合する結合手段と、
前記結合データを暗号化する暗号化手段と、
暗号化された前記結合データを前記相手機器に返信する第２送信手段と、
前記相手機器の第２送信手段から送信された暗号化結合データを受信する第２受信手段と、
受信した前記結合データを復号化する復号化手段と、
復号化された前記結合データをレスポンスデータに相当する第１分離データと前記データ転送鍵用の第２分離データに分離する分離手段と、
前記第１分離データと前記第１乱数生成手段で生成された前記第１乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、
前記第２乱数と前記第２分離データとを結合することで、前記データ転送鍵を生成するデータ転送鍵生成手段と、
前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする暗号化装置。
【請求項２２】　データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、
それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、
前記送信機は、
第１乱数を生成する第１乱数生成手段と、
前記第１乱数を暗号化する第１暗号化手段と、
暗号化された前記第１乱数を受信機に送信する第１送信手段とを備え、
前記受信機は、
暗号化された前記第１乱数を受信する第１受信手段と、
受信した前記第１乱数を復号化する第１復号化手段と、
第２乱数を生成する第２乱数生成手段と、
前記第１乱数と前記第２乱数を結合することで、結合データを生成する第１結合手段と、
前記結合データを暗号化する第２暗号化手段と、
暗号化された前記結合データを送信機に送信する第２送信手段とを備え、
前記送信機はさらに、

暗号化された前記結合データを受信する第２受信手段と、
受信した前記結合データを復号化する第２復号化手段と、
復号化された前記結合データを前記第１乱数に相当する第１分離データと前記第２乱数に相当する第２分離データとに分離する分離手段と、
前記第１乱数と前記第１分離データとを比較し、一致している場合に前記受信機を正当な機器と認証する第１比較手段と、
前記認証がなされた場合に前記第２分離データを暗号化する第３暗号化手段と、
暗号化された前記第２分離データを前記受信機に送信する第３送信手段と前記第１乱数生成手段で生成された記第１乱数と前記分離手段で得られた第２分離データとを結合することで、前記データ転送鍵を生成する第１データ転送鍵生成手段とを備え、
前記受信機はさらに、
暗号化された前記第２分離データを受信する第３受信手段と、
受信した前記第２分離データを復号化する第３復号化手段と、
復号化された前記第２分離データと前記第２乱数とを比較し、一致している場合に前記送信機を正当な機器と認証する第２比較手段と、
前記認証がなされた場合に前記第１復号化手段で得られた前記第１乱数と前記第２乱数生成手段で生成された第２乱数とを結合することで、前記データ転送鍵を生成する第２データ転送鍵生成手段とを備え、
前記送信機はさらに、
前記第１データ転送鍵生成手段で生成されたデータ転送鍵を用いて転送データを暗号化する第４暗号化手段と、
暗号化された転送データを前記受信機に送信する第４送信手段とを備え、
前記受信機はさらに、
暗号化された前記転送データを前記送信機から受信する第４受信手段と、
前記第２データ転送鍵生成手段で生成されたデータ転送鍵を用いて転送データを復号化する第４復号化手段とを備えることを特徴とする暗号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、秘密鍵を共有して暗号通信を行なう通信機器に備えられる暗号化装置に関し、特に、小さい回路規模で実現することができる暗号化装置に関する。
【０００２】
【従来の技術】通信路を介して通信されているデータが通信路上で不正にコピーされたり改変されることを防ぐことが必要となる場合が数多くある。例えば、映画など

の著作物がディジタル化されさらに情報圧縮され、さらに光ディスク上にディジタル記録されており、これが光ディスク再生装置により電気情報として取り出され、取り出されたデジタル情報が情報伸長装置により伸長され、映像音響再生装置により再生されるような場合である。

【０００３】ここで光ディスク再生装置と情報伸長装置は別々の機器として分離しており、その間がディジタル通信路によりデータ通信される場合、この通信データが著作者の許可なくディジタル情報記録装置により記録され、さらにディジタル情報複製装置により複製されるものであれば、その映画の著作物が不正に複製されることになり、著作権の侵害が起こる。従って通信路を介して通信されているデータが通信路上で不正にコピーされることを防がなければならない。機器内の回路や部品の仕様が一般には公開されないのに対し、データ通信のための電気的特性や信号形式は一般に公開される場合が多いので通信路におけるデータの不正コピーやそれに引き続くデータの改変が大きな問題になる。

【０００４】このような不正行為を排除して安全な通信を確保するための技術については従来より様々なものが知られている。最も代表的なものは相手認証技術を用いるものである。これは基本的にはデータを送出する側が受信する側の正当性を認証し、正当な受信者であることが確認できたときのみにデータを送信することで、デジタル著作物が不正な機器に受信されることを防止するものである。

【０００５】なお、この場合の受信者のように自らの正当性を証明する側を証明者と呼び、またこの場合の送信者のように相手の正当性を確認する側を認証者と呼ぶ。また、前述の光ディスク記録再生に関わる機器のような場合では、特定の機器の間で認証が成功するか否かということよりも、それら機器が光ディスク関連機器の業界によって定められた規格に準拠したものであるか否かが問題となる。従ってこのような場合では、「正当性」とは「所定の規格に準拠すること」を意味する。

（第１の従来技術）第１の具体的な従来技術として、国際標準規格ISO/IEC9798-2に記載される暗号技術を用いた一方向認証方法がある。

【０００６】この認証方法は証明者が認証鍵と呼ばれる秘密のデータを持つことを、その鍵自身を知らせることなく認証者に対して証明することを基本としている。そのためにまず認証者があるデータを選びこれを証明者に対して投げかける。この行為をチャレンジ、投げかけたデータをチャレンジデータと呼ぶ。これに対して証明者は、予め所有していた暗号変換と認証鍵を用いて前記チャレンジデータを暗号化する。そして、暗号化したデータを認証者に返す。この行為をレスポンス、そのデータをレスポンスデータを呼ぶ。

【０００７】このレスポンスデータを受信した認証者は、証明者が所有している暗号変換の逆変換である復号変換と認証鍵を共有しており、証明者から返信されてきたレスポンスデータをその認証鍵と復号変換を用いて復号化する。この結果が前記チャレンジデータと一致すれば受信者は正規の認証鍵を持つものと判断し、証明者の正当性を認証する。一方向認証とは一方の側がその正当性を他方に証明することを意味する。

【０００８】ここで、暗号変換Ｔとは、鍵データＳにより定まる平文集合から暗号文集合への写像である。平文をＸとしたとき暗号文を Ｔ（Ｓ，Ｘ）と書く。同じ鍵データＳにより定まる暗号文集合から平文集合への写像である逆変換ＴＩＮＶとの間には、

ＴＩＮＶ（Ｓ，Ｔ（Ｓ，Ｘ））＝Ｘ

の関係がある。これは平文Ｘを暗号変換し、これを逆変換すると元に戻ることを意味している。暗号変換の逆変換を復号変換と呼ぶ。暗号変換であるためには鍵Ｓの知識がないときに暗号文Ｔ（Ｓ，Ｘ）から平文Ｘを求めるのが困難であることが必要である。なお、慣例により暗号変換をＥ（Ｓ，　）、復号変換をＤ（Ｓ，　）と記す。

【０００９】図１１は、前記規格に記載されている認証方法の一例を示す図である。図１１では、第１の機器１１から第２の機器１２にデジタル著作物ｍｊを転送する場合が示されている。ここでは、第１の機器１１が第２の機器１２の正当性を確認する。以下この従来の一方向認証方法の動作を同図に示されたステップ番号に従って説明する。

【００１０】(1) 第１の機器１１は、乱数Ｒ１を生成する。そしてこれをチャレンジデータとして通信路を介して第２の機器１２に送信する。

(2) 第２の機器１２はこの乱数を受けとると、第２の機器１２に格納されている秘密の認証鍵Ｓを暗号鍵としてこの乱数を暗号化する。そしてその結果Ｃ１をレスポンスデータとして通信路を介して第１の機器１１に送信する。

【００１１】(3) 第１の機器１１はこのレスポンスデータを受け取ると、第１の機器１１に格納されている認証鍵Ｓを復号鍵としてこのレスポンスデータＣ１を復号化する。

(4) 第１の機器１１は、復号の結果ＲＲ１を第１の機器１１内に一時保管されている乱数Ｒ１と比較する。これが一致すれば第１の機器１１は第２の機器１２機器が同じ認証鍵Ｓを保有するものと考え、通信相手が正当なものであると認証する。一方、一致しなければ通信相手が正当なものではないものと判断して処理を中断する。

【００１２】(5) 第１の機器１１は第２の機器１２を正当なものと認証した後、デジタル著作物を通信路を介して第２の機器１２に送信する。もしも、第２の機器１２の代わりに認証鍵Ｓを有さない第３の機器が通信路に接続されている場合には、その第３の機器は上記ステップ

(2)で正しい値のデータＣ１を作成することができず、結果としてステップ(3)で復号の結果ＲＲ１が前記Ｒ１と一致しないため、ステップ(4)において第１の機器１１はデジタル著作物をその第３の機器に伝送しない。

【００１３】なお、第１の機器１１と第２の機器１２の間でいつも同じチャレンジデータとレスポンスデータが用いられるならば、そのことを知った不正な第３の機器が第２の機器１２になりすますことが考えられる。これを避けるために第１の機器１１からは毎回異なるチャレンジデータ（乱数）を送っている。

（第２の従来技術）ところで、上記第１の従来技術では、例えば認証の後、ハードディスク装置に記憶されている偽りのデータを正規の認証鍵を有する第２の機器１２に対して不正に送出することも可能である。この問題を解決するため、第１の機器１１が第２の機器１２の正当性を確認すると同時に、第２の機器１２も第１の機器１１の正当性を確認することが必要となる。

【００１４】また、双方の機器が認証した後にデジタル著作物を通信路を介して第２の機器１２に伝送している最中に、この通信路上のデータを抜きとり、これを例えばハードディスク装置に記憶することが考えられる。もちろんこのためには通信路上の信号の電気的特性やデータ形式などの知識が必要であるが、それらの知識は一般に特に秘密にされている情報ではないので、そのディジタル著作物の抜きとりは技術的に十分に可能である。そのため、認証だけでは不十分であり、認証が成功した後に、各機器間でランダムに生成した新たな鍵を共有し、その鍵を用いてデジタル著作物を暗号化して転送する暗号通信をすることが必要になる。なお、デジタル著作物等の転送すべきデータを暗号化するための秘密鍵を、以下、「データ転送鍵」と呼ぶ。

【００１５】以下、上記第１の従来技術である一方向認証を拡張し、双方向認証とデータ転送鍵の共有化と暗号通信とを行なう第２の従来技術を説明する。図１２は、この双方向認証を実現する装置の一例を示す。図１２には、第１の機器２１から第２の機器２２にデジタル著作物ｍｊを暗号化した後に転送する場合が示されている。

【００１６】以下この従来の双方向認証とデータ転送鍵の共有化の動作を同図に示されたステップ番号に従って説明する。

(1) 第１の機器２１は乱数Ｒ１を生成する。これは第１のチャレンジデータとしての意味を持つ。そしてこれを通信路を介して第２の機器２２に送信する。ここで乱数Ｒ２は第２の機器２２から第１の機器２１への第２のチャレンジデータとしての意味を持つ。つまり、暗号文Ｃ１は第１のチャレンジデータに対するレスポンスデータと第２のチャレンジデータの両方の意味を持つ。

【００１７】(2) 第２の機器２２は乱数Ｒ２を生成し、それと第１の機器２１から受けとった乱数Ｒ１とを結合することで結合データＲ１||Ｒ２を作成する。ここで記号"||"は双方のデータを桁方向に並べて結合することを示す。そして第２の機器２２の認証鍵Ｓを暗号鍵として、この結合データＲ１||Ｒ２を暗号化し、その暗号文Ｃ１を第１の機器２１に送信する。

【００１８】(3) 第１の機器２１は、第２の機器２２から受信した暗号文Ｃ１を認証鍵Ｓを復号鍵として復号化し、その結果の上位を分離データＲＲ１、下位を分離データＲＲ２とする。

(4) 第１の機器２１では、この分離データＲＲ１を第１の機器２１に一時記憶されている乱数Ｒ１と比較する。これが一致すれば通信相手が認証鍵Ｓを持っている正当な機器であると認証する。もしも一致しなければここで認証処理を中断する。

【００１９】(5) 第１の機器２１は、乱数Ｋを発生しこれをデータ転送鍵Ｋとして設定する。そして前記獲得した分離データＲＲ２とこのデータ転送鍵Ｋを結合した結合データＲＲ２||Ｋを第１の機器２１の認証鍵Ｓで暗号化して、その暗号文Ｃ２を第２の機器２２に送信する。

(6) 第２の機器２２は、第１の機器２１から受信した暗号文Ｃ２を認証鍵Ｓを用いて復号化し、その上位を分離データＲＲＲ２、下位を分離データＫＫとする。

【００２０】(7) 第２の機器２２は、この分離データＲＲＲ２を第２の機器２２に一時記憶されている乱数Ｒ２と比較する。これが一致すれば通信相手が認証鍵Ｓを持っている正当な機器であると認証する。もしも一致しなければ、ここで認証処理を中断する。一方、復号化した分離データＫＫをデータ転送鍵ＫＫとして設定する。

【００２１】(8) 第１の機器２１は、前記データ転送鍵Ｋを用いてデジタル著作物を暗号化し、通信路を介して第２の機器２２に送信する。

(9)第２の機器２２ではこれを前記データ転送鍵ＫＫを用いて復号化し、もとのデジタル著作物を獲得する。ここで、もしも第１の機器２１が正規の認証鍵Ｓを有し、第２の機器２２が正規の認証鍵を有していない場合には、ステップ(4)で第１の機器２１は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。また第１の機器２１が正規の認証鍵を有しておらず、第２の機器２２は正規の認証鍵を有している場合には、ステップ(7)において第２の機器２２は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。このようにしてデジタル著作物が不正な機器に流出することを防止すると同時に不正な機器から正当な機器に流入することも防止することができる。

【００２２】さらに、第１の機器２１も第２の機器２２も正当な認証鍵を有している場合において前記認証処理が完了しステップ(8)においてデジタル著作物が通信路上を伝送されている際に、もし、そのデジタル著作物が電気的にコピーされ、ディジタル蓄積装置に蓄積された場合であっても、そのディジタル著作物は暗号化されているので、無意味なデジタルデータとなっており、元の

デジタル著作物は有効に保護される。

【００２３】以上のように、暗号技術を用いた双方向認証が首尾よく行われるには、第１の機器２１及び第２の機器２２の内部に格納されている認証鍵が不正を行おうとするものに容易に分からないことが必須の条件となる。また、チャレンジデータのための乱数の生成部やデータ転送鍵Ｋの生成部が外部からアクセス不可なこと、変更できないことが必要である。

【００２４】それら構成要素の秘匿性を確保する最も効果的な方法は、上記の認証やデータ転送鍵の共有化及び暗号通信を行う部分をＩＣとして実現する方法である。ＩＣを解析するには一般に多大な労力がかかるので、認証鍵などが容易には解読されないからである。

【００２５】

【発明が解決しようとする課題】ところが、上記の第２従来技術における第１の機器２１をＩＣで実現するためには、そのようなＩＣ（以下、「暗号化ＩＣ」という。）は次の部分を備えることが必要である。

・乱数Ｒ１を生成する乱数生成部
・暗号文Ｃ１を復号化するための復号部
・認証鍵Ｓを格納する部分
・乱数Ｒ１と分離データＲＲ１を比較するための比較部
・データ転送鍵Ｋを生成するための乱数生成部
・分離データＲＲ２とデータ転送鍵Ｋを結合して暗号化するための暗号部
・データ転送鍵Ｋを格納する部分
・データ転送鍵Ｋを用いてデジタル著作物を暗号化する暗号部

第２の機器２２についてもこれと同程度の規模のハードウェアが必要である。

【００２６】このように、上記従来の認証方式をＩＣで実現したのでは、２つの乱数生成部、２つの変換部（復号部と暗号部）非常に多くの機能を持たなければならないために、回路規模が大きくなり結局機器のコストアップにつながるという問題点を有する。また、上記第２従来技術ではデータを暗号化するためのデータ転送鍵Ｋは第１の機器２１が生成しているが、相互認証が必要とされるのと同じ理由により、この鍵は双方の機器が生成した値を反映するほうが望ましい。

【００２７】以上説明したように、機器間の回線を保護するためには、認証等の機能やそのための秘密の情報をＩＣに封じ込めて実現する方法が効果的である。しかし、従来の方法において、相互認証の部分、データ転送鍵の共有化の部分及びデータ暗号化の部分をすべて１つのＩＣで実現するのでは、そのＩＣの規模は非常に大きくなってしまい、コストアップにつながる。

【００２８】そこで、本発明は、規模の小さな暗号化ＩＣを備え、機器間通信の安全性を確保するための必要最小限の機能を有する暗号化装置を提供することを第１の目的とする。ここで暗号化ＩＣは次の機能を有する。

(1) 認証鍵を安全に格納する。その鍵は外部からのアクセスにより書き換え及び読み出しがなされない。

【００２９】(2) データ転送鍵を安全に共有する。その鍵は外部からのアクセスにより書き換え及び読み出しがなされない。

(3) 但し、通信システムの安全性に関連しない部分を暗号化ＩＣに備えないことにより、暗号化ＩＣの規模を最小とする。また、本発明の第２の目的は、規模の小さな暗号化ＩＣを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムを提供することである。

【００３０】

【課題を解決するための手段】上記第１の目的を達成するために本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、前記データ転送鍵の共有化のための第１乱数を生成する第１乱数生成手段と、前記第１乱数生成手段により生成された第１乱数を保持する第１乱数保持手段と、前記第１乱数生成手段により生成された第１乱数を前記暗号通信の相手機器に送信する第１送信手段と、前記第１乱数保持手段に保持された第１乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、前記第１乱数生成手段、前記第１乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、１個のＩＣ内の回路で実現され、前記第１乱数保持手段は、前記ＩＣの外部からアクセスできない領域に前記第１乱数を保持することを特徴とする。

【００３１】これにより、データ転送鍵の生成に直接関連する第１乱数は外部からアクセスできない暗号化ＩＣの内部に保持されるので、時変のデータ転送鍵は各機器に安全に共有され、暗号通信が行われる。また、暗号化ＩＣは、機器間通信の安全性を確保するための必要最小限の機能を持つので、小さな回路で実現することができる。

【００３２】また、上記第２の目的を達成するために本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞれ、チャレンジデータ用の第１乱数を生成する第１乱数生成手段と、前記データ転送鍵用の第２乱数を生成する第２乱数生成手段と、前記第１乱数と前記第２乱数を結合する結合手段と、前記結合データを暗号化する暗号化手段と、暗号化された前記結合データを前記相手機器に送信する第１送信手段と、前記相手機器の第１送信手段から送信された暗号化された結合データを受信する第１受信手段と、受信した前記結合データを復号化する復号化手段と、復号化された前記結合

データをレスポンスデータに相当する第１分離データと前記データ転送鍵用の第２分離データに分離する分離手段と、前記第１分離データをレスポンスデータとして前記相手機器に返信する第２送信手段と、前記相手機器の第２送信手段から返信された第１分離データを受信する第２受信手段と、受信した前記第１分離データと前記第１乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、前記第２乱数と前記第２分離データとを結合することで、前記データ転送鍵を生成するデータ転送鍵生成手段と、前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする。

【００３３】これにより、送信機及び受信機間で相互認証が行われると共にデータ転送鍵が生成されること、データ転送鍵の生成に直接関連する乱数はそのままでは送受信されないこと、及び、データ転送鍵の生成に直接関連する２つの乱数はそれぞれ送信機及び受信機から提供されたものであることから、規模の小さな暗号化ＩＣを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムが実現される。

【００３４】

【発明の実施の形態】

（実施の形態１）図１は、本発明に係る暗号化装置を備えた第１の機器と第２の機器間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行う実施の形態１における処理シーケンスを示す図である。

【００３５】図１では、第１の機器５１から第２の機器５２にデジタル著作物ｍｊを転送する場合が示されている。なお、図１には、各機器５１、５２が備える暗号化装置だけが示されており、暗号化装置と直接に関連しない他の構成要素（送受信部やデジタル著作物の処理系等）は省略されている。第１の機器５１に備えられた本発明に係る暗号化装置は、大きく分けてＭＰＵ５３と第１の暗号化ＩＣ５４とから構成される。

【００３６】ＭＰＵ５３は、この暗号化装置に固有の制御プログラムを保持するＲＯＭとその制御プログラムを実行する汎用マイクロプロセッサとＲＡＭ等からなり、データ転送鍵の共有化に直接的には関与しない処理（図中のステップ(1)、(7)）を行なう。第１の暗号化ＩＣ５４は、１チップの半導体ＩＣであり、データ転送鍵の共有化に直接的に関与する処理（図中のステップ(3),(5),(9),(11)）を行なう。

【００３７】同様に、第２の機器５２に備えられた本発明に係る暗号化装置も、大きく分けてＭＰＵ５５と第２の暗号化ＩＣ５６とから構成される。ＭＰＵ５５は、この暗号化装置に固有の制御プログラムを保持するＲＯＭとその制御プログラムを実行する汎用マイクロプロセッサとＲＡＭ等からなり、データ転送鍵の共有化に直接的には関与しない処理（図中のステップ(2)、(8)）を行なう。

【００３８】第２の暗号化ＩＣ５６は、１チップの半導体ＩＣであり、データ転送鍵の共有化に直接的に関与する処理（図中のステップ(4),(6),(10),(12)）を行なう。なお、この実施の形態においては、データ暗号化規格（DES:Data EncryptionStandard）に準拠した６４ビットブロック暗号アルゴリズムＥとその逆変換アルゴリズムＤを用いている。以降では暗号アルゴリズムＥを用いる変換を「暗号化」、逆変換アルゴリズムＤを用いる変換を「復号化」と称する。

【００３９】また、第１の暗号化ＩＣ５４は暗号アルゴリズムＥだけを、第２の暗号化ＩＣ５６は逆変換アルゴリズムＤだけを備える。これは、各暗号化ＩＣ５４、５６の規模を削減することと、安全性のためである。以下、図１に示されたステップ番号に従って、実施の形態１における暗号化装置の動作を説明する。

【００４０】(1) 第１の機器５１のＭＰＵ５３において乱数Ｒ１（３２ビット）を生成して、記憶するとともに第１の暗号化ＩＣ５４に渡す。

(2) ステップ(1)と同様に、第２の機器５２のＭＰＵ５５において乱数Ｒ２（３２ビット）を生成して、記憶するとともに第２の暗号化ＩＣ５６に送信する。

【００４１】(3) 第１の暗号化ＩＣ５４において、乱数Ｒ３（３２ビット）を生成、外部よりアクセスできない領域に格納する。そして、前記ＭＰＵで生成した乱数Ｒ１と前記乱数Ｒ３を結合してＥ関数で暗号化する。ここで、記号"||"は２つの乱数を桁方向に結合して６４ビット（乱数Ｒ１を上位３２ビット、乱数Ｒ３を下位３２ビット）とすることを示している。また、暗号化には第１の暗号化ＩＣ５４及び第２の暗号化ＩＣ５６で予め共通に保持している秘密の認証鍵Ｓを用いる。第１の暗号化ＩＣ５４は、第１の機器５１の送信部（図では示していない）を介して上記暗号結果Ｃ１を第２の機器５２に送信する。

【００４２】(4) ステップ(3)と同様に、第２の暗号化ＩＣ５６において、乱数Ｒ４（３２ビット）を生成して、外部よりアクセスできない領域に格納する。前記ＭＰＵで生成した乱数Ｒ２と前記乱数Ｒ４を結合して逆変換アルゴリズムＤで復号化する。復号には前記認証鍵Ｓを用いる。第２の暗号化ＩＣ５６は、第２の機器５２の送信部（図では示していない）を介して復号結果Ｃ２（６４ビット）を第１の機器５１に送信する。

【００４３】(5) 第１の暗号化ＩＣ５４において、前記第２の機器５２から受信した復号文Ｃ２を前記Ｅ関数を用いて前記認証鍵Ｓで暗号化する。そして、得られた６４ビットをその上位３２ビットである分離データＲＲ２と下位３２ビットである分離データＲＲ４に分離する。さらに、分離データＲＲ２は第１の機器５１の送信部を介して第２の機器５２に送信し、一方、分離データＲＲ４は外に出さずに第１の暗号化ＩＣ５４内の外部からア

クセスできない領域に格納する。

【００４４】なお、第１の暗号化ＩＣ５４及び第２の暗号化ＩＣ５６が互いに正規なものであり同じ認証鍵Ｓを保持している場合には、前記分離データＲＲ２は前記第２の機器５２のＭＰＵ５５が生成した乱数Ｒ２と一致し、前記分離データＲＲ４は前記第２の暗号化ＩＣ５６が内部に格納している乱数Ｒ４と一致する。

(6) ステップ(5)と同様に、第２の暗号化ＩＣ５６において、前記第１の暗号化ＩＣ５４から受信した暗号文Ｃ１を前記逆変換アルゴリズムＤを用いて前記認証鍵Ｓで復号化する。そして、得られた６４ビットをその上位３２ビットである分離データＲＲ１と下位３２ビットである分離データＲＲ３に分離する。さらに、分離データＲＲ１は第２の機器５２の送信部を介して第１の機器５１に送信し、一方、分離データＲＲ３は外に出さずに第２の暗号化ＩＣ５６内の外部からアクセスできない領域に格納する。

【００４５】なお、第１の暗号化ＩＣ５４及び第２の暗号化ＩＣ５６が互いに正規なものであり同じ認証鍵Ｓを保持している場合には、前記分離データＲＲ１は前記乱数Ｒ１と一致し、前記分離データＲＲ３は前記乱数Ｒ３と一致する。

(7) 第１の機器５１のＭＰＵ５３において前記ステップ(1)で記憶していた乱数Ｒ１と前記第２の機器５２から受信した分離データＲＲ１とを比較し、一致している場合には、第２の暗号化ＩＣ５６及びそれを備えた第２の機器５２を正当な機器と認証する。

【００４６】(8) ステップ(7)と同様に、第２の機器５２のＭＰＵ５５において前記ステップ(2)で記憶していた乱数Ｒ２と前記第２の機器５２から受信した分離データＲＲ２とを比較し、一致している場合には、第１の暗号化ＩＣ５４及びそれを備えた第１の機器５１を正当な機器と認証する。

(9) 第１の暗号化ＩＣ５４において、前記ステップ(3)で記憶しておいた乱数Ｒ３と前記分離データＲＲ４を結合することでデータ転送鍵Ｋを作成する。ここでは、乱数Ｒ３を上位の３２ビット、分離データＲＲ４を下位の３２ビットとするデータ転送鍵Ｋ（６４ビット）を生成する。なお、このデータ転送鍵Ｋは、２つの乱数の結合であるので、時変、即ち、新たにランダムに生成された鍵と言える。

【００４７】(10) ステップ(9)と同様に、第２の暗号化ＩＣ５６において、前記分離データＲＲ３と前記ステップ(4)で記憶しておいた乱数Ｒ４を結合することでデータ転送鍵Ｋを生成する。ここでは、上記分離データＲＲ３を上位の３２ビット、上記ステップ(4)で記憶しておいた乱数Ｒ４を下位の３２ビットとするデータ転送鍵Ｋ（６４ビット）を生成する。このデータ転送鍵も時変の鍵である。

【００４８】なお、ステップ(7)及びステップ(8)での相互の認証が成功した場合には、ステップ(3)で生成された乱数Ｒ３とステップ(6)で得られた分離データＲＲ３とは一致し、ステップ(4)で生成された乱数Ｒ４とステップ(5)で得られた分離データＲＲＲ４とは一致することになるので、結果的に、ステップ(9)及びステップ(10)それぞれで生成されるデータ転送鍵Ｋは一致することになる。

【００４９】(11) 第１の機器５１の第１の暗号化ＩＣ５４において、ＭＰＵ５３から送られてくるブロック化されたデジタル著作物ｍｊ（６４ビット）を上記ステップ(9)で得られたデータ転送鍵Ｋを用いて暗号化し、得られた暗号文Ｃｊを第２の機器５２に送信する処理を、転送すべき全てのデジタル著作物を送信し終えるまで繰り返す。

【００５０】(12) ステップ(11)に対応して、第２の機器５２の第２の暗号化ＩＣ５６において、第１の機器５１が送信した暗号化された上記デジタル著作物Ｃｊ（６４ビット）を受信し、上記ステップ(10)で得られたデータ転送鍵Ｋを用いて復号化し、得られたデジタル著作物ｍｍｊをＭＰＵ５５に送る。この復号化は上記デジタル著作物Ｃｊが第１の機器５１から送信されてくる限り繰り返す。

【００５１】このようにして、実施の形態１の暗号化装置により、第１の機器５１と第２の機器５２間で相互認証とデータ転送鍵Ｋの共有化とデータの暗号通信とが行われる。以上の説明から明らかなように、上記実施の形態１の暗号化装置は、以下の特徴を有する。

【００５２】第１の特徴は、データ転送鍵Ｋは暗号化ＩＣの内部に安全に保護されていることである。具体的には、第１の機器５１が備える暗号化装置であれば、データ転送鍵Ｋを生成するために直接的に用いられた２つのデータ、即ち、乱数Ｒ３と分離データＲＲ４は以下の条件を満たす。

・乱数Ｒ３は、第１の暗号化ＩＣ５４の内部で生成され、外部に出力されておらず、かつ、外部から読めない領域に保持されている。

【００５３】・分離データＲＲ４は、第１の暗号化ＩＣ５４の内部で生成（分離生成）され、外部に出力されておらず、かつ、外部から読めない領域に保持されている。これらのことにより、データ転送鍵Ｋは暗号化ＩＣ内に保護されるので、暗号アルゴリズムＥ及び逆変換アルゴリズムＤとして公開されているものを採用したとしても、第１の機器５１及び第２の機器５２間における暗号通信の安全性は保証される。

【００５４】第２の特徴は、暗号化ＩＣ内に納められる回路は、必要最低限のものに留められていることである。具体的には、第１の機器５１が備える暗号化装置であれば、以下の処理は、第１の暗号化ＩＣ５４の外の回路、即ち、ＭＰＵ５３によって実現されている。

・乱数Ｒ１の生成

・乱数Ｒ１と分離データＲＲ１との比較

つまり、第１の暗号化ＩＣ５４の回路規模が不必要に大きくならないように配慮されている。これら２つの処理は、相手機器の認証に関するものであり、データ転送鍵Ｋの生成に直接的には関与していない。従って、たとえ、これら処理がＩＣ外で実現されていることを利用して不正をしようとしても、第１の機器５１に利益をもたらすような不正をはたらくことは不可能である。なお、第２の機器５２からのチャレンジデータＣ２に対するレスポンスデータＲＲ２の作成は暗号化ＩＣ内で行っている。

【００５５】図２は、第１の暗号化ＩＣ５４のハードウェア構成を示すブロック図である。第２の暗号化ＩＣ５６も同程度のハードウェア規模で実現できる。外部Ｉ／Ｆ部６１は、この第１の暗号化ＩＣ５４の内部回路に外部からアクセスするための唯一の入出力ポートである。乱数生成部６０は、３２ビットの乱数Ｒ３を生成する。

【００５６】乱数格納部６２は、乱数生成部６０で生成された乱数Ｒ３を保持する記憶回路である。結合部６３は、乱数格納部６２に格納された乱数Ｒ３を下位３２ビットとし、外部Ｉ／Ｆ部６１を介して入力された３２ビットのデータＲ１を上位３２ビットとして結合する。

【００５７】認証鍵Ｓ格納部６４は、予め与えられた認証鍵Ｓを保持する記憶回路である。スイッチ６５、６６は、それぞれ６４ビット幅の３入力１出力マルチプレクサ、６４ビット幅の２入力１出力マルチプレクサである。Ｅ関数６７は、暗号アルゴリズムＥに基づく暗号化回路である。スイッチ６８は、６４ビット幅の１入力３出力デマルチプレクサである。

【００５８】分離部６９は、スイッチ６８から出力された６４ビットデータを上位３２ビットＲＲ２と下位３２ビットＲＲ４に分離する。データ転送鍵Ｋ生成部５９は、乱数格納部６２に格納された乱数Ｒ３を上位３２ビットとし、分離部６９で分離された分離データＲＲ４を下位３２ビットとして結合することで、データ転送鍵Ｋを生成する。

【００５９】データ転送鍵Ｋ格納部７０は、データ転送鍵Ｋ生成部５９で生成されたデータ転送鍵Ｋを保持する記憶回路である。次に、この図２に示された各構成要素が図１に示された各ステップにおいていかに動作するのかを示す。図１のステップ(3)においては、乱数生成部６０は乱数Ｒ３を生成して乱数格納部６２に格納し、結合部６３はその乱数Ｒ３と外部Ｉ／Ｆ部６１を介して入力される乱数Ｒ１とを結合し、スイッチ６５を介してＥ関数６７に送る。Ｅ関数６７は、認証鍵Ｓ格納部６４からスイッチ６６を介して認証鍵Ｓを受け取り、それを用いて結合部６３から出力された結合データＲ１||Ｒ３を暗号化し、その結果Ｃ１をスイッチ６８及び外部Ｉ／Ｆ部６１を介して第２の機器５２に出力する。

【００６０】図１のステップ(5)及び(9)においては、外部Ｉ／Ｆ部６１を介して入力される復号文Ｃ２はスイッチ６５を経てＥ関数に入力される。Ｅ関数６７は、認証鍵Ｓ格納部６４から認証鍵Ｓを受け取り、それを用いて復号文Ｃ２を暗号化し、スイッチ６８を介して分離部６９に送る。分離部６９は、それを分離データＲＲ２と分離データＲＲ４に分離し、分離データＲＲ２は外部Ｉ／Ｆ部６１を介して外部に出力し、分離データＲＲ４はデータ転送鍵Ｋ生成部５９に送る。データ転送鍵Ｋ生成部５９は、乱数格納部６２に格納されていた乱数Ｒ３と分離部６９から送られてきた分離データＲＲ４とを結合することでデータ転送鍵Ｋを生成した後に、データ転送鍵Ｋ格納部７０に格納する。

【００６１】図１のステップ(11)においては、Ｅ関数６７は、外部Ｉ／Ｆ部６１及びスイッチ６５を介して入力されるデジタル著作物ｍｊをデータ転送鍵Ｋ格納部７０に格納されたデータ転送鍵Ｋを用いて暗号化し、その結果Ｃｊをスイッチ６８及び外部Ｉ／Ｆ部６１を介して第２の機器５２に出力する。なお、実施の形態１では、乱数や暗号文等の具体的なビット長やデータ構成を示したが、本発明はそれらに限定されるものではない。例えば、上記ステップ(5)において３２ビットの乱数Ｒ１とＲ２を結合して６４ビットとし、これを６４ビット暗号関数Ｅに入力して６４ビットの暗号文Ｃ１を求めている。この部分は、例えば、各乱数を６４ビットとし、暗号関数Ｅによる暗号化を２回繰り返すことで１２８ビットの暗号文Ｃ１を生成する方式としてもよい。ただしこの場合には暗号文Ｃ１から乱数Ｒ１に関する部分とＲ２に関する部分が容易に切り離せないことが必要である。その方法の１つとしてはＣＢＣモードのように連鎖を伴う暗号の方法がある。ＣＢＣモードについては、池野信一、小山謙二共著「現代暗号理論」電子通信学会１９８６年のｐ７０に詳しい。

【００６２】また、実施の形態１では第１の暗号化ＩＣ５４は暗号関数Ｅだけを、第２の暗号化ＩＣ５６はその逆関数Ｄだけを備えることにより、ハードウェア規模を削減しているが、そのこと自体は、上述したように本発明の本質ではない。つまり、それら暗号化ＩＣ５４、５６に許容される回路規模や暗号化アルゴリズムの種類等との関連において決定すればよい事項であり、例えば、それぞれが暗号アルゴリズムＥと逆変換アルゴリズムＤの両方を所有し、乱数の暗号化に暗号アルゴリズムＥを、相手機器から送付された情報の復号に逆変換アルゴリズムＤを用いてもよい。本発明は、少なくともデータ転送鍵Ｋの生成に直接関わる構成要素をＩＣ化することで秘密通信の安全性を確保している点に特徴があるからである。

【００６３】また、実施の形態１において、例えば、ステップ(1)での乱数Ｒ１の生成を第１の暗号化ＩＣ５４内で行ってもよい。このことにより、第１の暗号化ＩＣ５４を暗号解読器として用いる可能性をなくし、より安

全な暗号化装置とすることができる。つまり、実施の形態１では、乱数Ｒ１は第１の暗号化ＩＣ５４の外部で生成され、この乱数Ｒ１に基づいて第１の暗号化ＩＣ５４は暗号文Ｃ１を出力する。この暗号文Ｃ１は、第１の暗号化ＩＣ５４の内部で生成された乱数Ｒ３の影響を受けているが、もし乱数Ｒ３が十分にランダムな値でない場合には、第１の暗号化ＩＣ５４を暗号解読器として悪用することが可能になってしまう。従って、乱数Ｒ１の生成を第１の暗号化ＩＣ５４内で行うことで、以上述べた攻撃の可能性がなくなり、この暗号化装置はより安全なものになる。

（実施の形態２）次に、図１に示された実施の形態１でのステップの変形例として、実施の形態２を示す。その目的や効果は実施の形態１と同じである。またハードウェア規模としても図２に示された実施の形態１と同程度である。実施の形態１ではチャレンジデータを暗号化しないでレスポンスデータを暗号化して通信したが、実施の形態２ではチャレンジデータを暗号化しレスポンスデータを暗号化しないで通信する。実施の形態１と相違する点を中心に説明する。

【００６４】図３は、本発明に係る暗号化装置を備えた第１の機器７１と第２の機器７２間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行う実施の形態２における処理シーケンスを示す図である。図３では、第１の機器７１から第２の機器７２にデジタル著作物ｍｊを転送する場合が示されている。

【００６５】ＭＰＵ７３、第１の暗号化ＩＣ７４、ＭＰＵ７５及び第２の暗号化ＩＣ７６は、実施の形態１におけるＭＰＵ５３、第１の暗号化ＩＣ５４、ＭＰＵ５５及び第２の暗号化ＩＣ５６に対応し、処理手順の相違を除いて、ハードウェア構成等については実施の形態１の場合と同様である。以下、図３に示されたステップ番号に従って、実施の形態２における暗号化装置の動作を説明する。

【００６６】(1) 第１の機器７１のＭＰＵ７３において乱数Ｒ１（３２ビット）を生成して、記憶するとともに第１の機器７１の送信部（図では示してない）を介して、第２の機器７２に送信する。第２の機器７２ではこれを第２の暗号化ＩＣ７６に渡す。

(2) ステップ(1)と同様に、第２の機器７２のＭＰＵ７５において乱数Ｒ２（３２ビット）を生成して、記憶するとともに第２の機器７２の送信部（図では示してない）を介して、第１の機器７１に送信する。第１の機器７１ではこれを第１の暗号化ＩＣ７４に渡す。

【００６７】(3) 第１の暗号化ＩＣ７４において、乱数Ｒ３（３２ビット）を生成して、外部よりアクセスできない領域に格納する。前記第２の機器７２から受信した乱数Ｒ２と前記乱数Ｒ３とを結合してＥ関数で暗号化する。暗号化には第１の暗号化ＩＣ７４及び第２の暗号化ＩＣ７６で予め共通に保持している秘密の認証鍵Ｓを用いる。第１の暗号化ＩＣ７４は、暗号化結果Ｃ１（６４ビット）を第２の機器７２に送信する。

【００６８】(4) ステップ(3)と同様に、第２の暗号化ＩＣ７６において、乱数Ｒ４（３２ビット）を生成して、外部よりアクセスできない領域に格納する。前記第１の機器７１から受信した乱数Ｒ１と前記乱数Ｒ４を結合して逆変換アルゴリズムＤで復号化する。復号には前記認証鍵Ｓを用いる。第２の暗号化ＩＣ７６は、復号結果Ｃ２（６４ビット）を第１の機器７１に送信する。

【００６９】(5) 第１の暗号化ＩＣ７４において、前記第２の暗号化ＩＣ７６から受信した復号文Ｃ２を前記Ｅ関数を用いて前記認証鍵Ｓで暗号化する。その結果の６４ビットデータのうち上位３２ビットを分離データＲＲ１，下位３２ビットを分離データＲＲ４とする。そして分離データＲＲ１は第１の機器７１のＭＰＵ７３に渡し、一方分離データＲＲ４は外に出さずに第１の暗号化ＩＣ７４内の外部からアクセスできない領域に格納する。

【００７０】なお、第１、第２の暗号化ＩＣ７６が互いに正規なものであり同じ認証鍵Ｓを保持している場合には、前記分離データＲＲ１は前記第１の機器７１のＭＰＵ７３が生成した乱数Ｒ１と同じになり、前記分離データＲＲ４は第２の暗号化ＩＣ７６が生成した乱数Ｒ４と同じになる。

(6) ステップ(6)と同様に、第２の暗号化ＩＣ７６において、前記第１の暗号化ＩＣ７４から受信した暗号文Ｃ１を前記逆変換アルゴリズムＤを用いて前記認証鍵Ｓで復号化する。その結果の６４ビットデータの上位３２ビットを分離データＲＲ２、下位３２ビットを分離データＲＲ３とする。そして分離データＲＲ２は第２の機器７２のＭＰＵ７５に渡し、一方分離データＲＲ３は外に出さずに第２の暗号化ＩＣ７６内の外部からアクセスできない領域に格納する。

【００７１】なお、第１、第２の暗号化ＩＣ７６が互いに正規なものであり同じ認証鍵Ｓを保持している場合には、前記分離データＲＲ２は前記第２の機器７２のＭＰＵ７５が生成した乱数Ｒ２と同じになり、前記分離データＲＲ３は第１の暗号化ＩＣ７４が生成した乱数Ｒ３と同じになる。

(7) 第１の機器７１のＭＰＵ７３において前記記憶していたＲ１と前記第１の暗号化ＩＣ７４から受け取った分離データＲＲ１を比較して一致している場合には、第２の暗号化ＩＣ７６及び第２の暗号化ＩＣ７６が含まれた第２の機器７２を正当な機器と認証する。

【００７２】(8) ステップ(8)と同様に、第２の機器７２のＭＰＵ７５において前記記憶していたＲ２と前記第２の暗号化ＩＣ７６から受け取った分離データＲＲ２を比較して一致している場合には、第１の暗号化ＩＣ７４及び第１の暗号化ＩＣ７４が含まれた第１の機器７１を正当な機器と認証する。

(9) 第１の暗号化ＩＣ７４内で前記乱数Ｒ３と前記分離データＲＲ４を用いてデータ転送鍵Ｋを作成する。図では双方の結合をデータ転送鍵Ｋ（６４ビット）としている。

【００７３】(10) ステップ(10)と同様に、第２の暗号化ＩＣ７６内で前記分離データＲＲ３と前記乱数Ｒ４を用いて第１の暗号化ＩＣ７４と同様にデータ転送鍵Ｋを作成する。図では双方の結合をデータ転送鍵Ｋ（６４ビット）としている。

(11) 第１の機器７１の第１の暗号化ＩＣ７４において、ＭＰＵ７３から送られてくるブロック化されたデジタル著作物ｍｊ（６４ビット）を上記ステップ(9)で得られたデータ転送鍵Ｋを用いて暗号化し、得られた暗号文Ｃｊを第２の機器７２に送信する処理を、転送すべき全てのデジタル著作物を送信し終えるまで繰り返す。

【００７４】(12) ステップ(11)に対応して、第２の機器７２の第２の暗号化ＩＣ７６において、第１の機器７１が送信した暗号化された上記デジタル著作物Ｃｊ（６４ビット）を受信し、上記ステップ(10)で得られたデータ転送鍵Ｋを用いて復号化し、得られたデジタル著作物ｍｍｊをＭＰＵ７５に送る。この復号化は上記デジタル著作物Ｃｊが第１の機器７１から送信されてくる限り繰り返す。

【００７５】このようにして、実施の形態２の暗号化装置により、実施の形態１の場合と同様に、第１の機器７１と第２の機器７２間で相互認証とデータ転送鍵Ｋの共有化とデータの暗号通信とが行われる。なお、上述したように、本実施の形態の暗号化装置と実施の形態１のものとはハードウェア構成において一致し、処理手順、即ち、各ハードウェア構成要素の接続と実行順序が異なるだけである。従って、本実施形態の暗号化装置の特徴やその変形例については、実施の形態１の場合と同様のことが言える。

（実施の形態３）以上の実施の形態１及び２の暗号化装置には以下の共通点がある。

(1)双方の機器においてそれぞれ２つの乱数が生成され、その一方は認証用にのみ使用され、他の一方はデータ転送鍵Ｋの生成用にのみ使用される。

(2)データ転送鍵Ｋの生成に使用される乱数はそのままの形では暗号化ＩＣの外部に出力されることはなく、一方、認証用に使用される乱数は暗号化ＩＣの外部に出力されて公開される。

【００７６】これに対して、次に説明する実施の形態３の暗号化装置は、乱数を一つだけ生成し、それを認証用とデータ転送鍵の生成用の両方の目的に使用する。これは、実施の形態１及び２に比べて、暗号化ＩＣ内での乱数生成の負担を軽減するためである。また、暗号化ＩＣの内部において認証のための乱数生成と比較処理を行う。即ち、実施の形態１及び２と相違し、データ転送鍵の生成のみならず認証処理も含めて暗号化ＩＣの内部回路で行う。これは、上述したように、暗号化ＩＣを暗号解読のために用いるという悪用に対処するためであり、暗号通信の安全性を高めることができる。

【００７７】図４は、本発明に係る暗号化装置を備えた第１の機器７１と第２の機器７２間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行う実施の形態３における処理シーケンスを示す図である。図４では、第１の機器８１から第２の機器８２にデジタル著作物ｍｊを転送する場合が示されている。

【００７８】なお、本実施の形態においても、実施の形態１及び２と同様に、各機器８１、８２に備えられた本発明に係る暗号化装置は、大きく分けてＭＰＵ８３、８５と暗号化ＩＣ８４、８６とから構成される。しかし、ＭＰＵ８３、８５はデジタル著作物ｍｊを暗号化ＩＣ８４、８６に渡すだけの機能を果たすので、実質的には、本発明に係る暗号化装置は暗号化ＩＣ８４、８６のみから構成されると言える。

【００７９】第１の暗号化ＩＣ８４及び第２の暗号化ＩＣ８６は、実の形態１及び２と同様、１チップの半導体ＩＣである。以下、図４に示されたステップ番号に従って、実施の形態３における暗号化装置の動作を説明する。

(1) 第１の暗号化ＩＣ８４において乱数Ｒ１を生成して記憶するとともに、これをＥ関数で暗号化して第１の機器８１の送信部（図では示してない）を介して、暗号文Ｃ１を第２の機器８２に送信する。暗号化には第２の暗号化ＩＣ８６と予め共通に保持している秘密の認証鍵Ｓを用いる。第２の機器８２では受信した暗号文Ｃ１を第２の暗号化ＩＣ８６に渡す。

【００８０】(2) 第２の暗号化ＩＣ８６では受信した暗号文Ｃ１を逆変換アルゴリズムＤで復号化し復号文ＲＲ１を得る。第１の暗号化ＩＣ８４及び第２の暗号化ＩＣ８６が正規のものである場合にはこの復号文ＲＲ１は前記乱数Ｒ１と一致する。

(3) 第２の暗号化ＩＣ８６において乱数Ｒ２を生成して記憶すると共に、これを前記復号文ＲＲ１と結合して前記逆変換アルゴリズムＤで復号化する。復号には前記認証鍵Ｓを用いる。第２の暗号化ＩＣ８６は復号文Ｃ２を第２の機器８２の送信部（図では示してない）を介して、第１の機器８１に送信する。第１の機器８１ではこれを第１の暗号化ＩＣ８４に渡す。

【００８１】(4) 第１の暗号化ＩＣ８４においては、前記復号文Ｃ２を前記Ｅ関数で暗号化し、その結果を分離データＲＲＲ１と分離データＲＲ２に分離する。なお分離データＲＲＲ１は正当な機器でのやり取りの場合であれば、前記復号文ＲＲ１及び乱数Ｒ１と一致する。また分離データＲＲ２は前記乱数Ｒ２と一致する。

(5) 第１の暗号化ＩＣ８４内において、前記ステップ(1)で記憶していた乱数Ｒ１と前記分離データＲＲＲ１とを比較し、一致する場合には第２の暗号化ＩＣ８６及

び第２の暗号化ＩＣ８６を含んだ第２の機器８２の正当性を認証する。

【００８２】(6) 第１の暗号化ＩＣ８４において、前記分離データＲＲ２を前記Ｅ関数で暗号化し、第２の機器８２に送信する。第２の機器８２はこの暗号文Ｃ３を第２の暗号化ＩＣ８６に渡す。

(7) 第２の暗号化ＩＣ８６において、前記暗号文Ｃ３を前記逆変換アルゴリズムＤで復号化し、復号文ＲＲＲ２を得る。

【００８３】(8) 第２の暗号化ＩＣ８６において、前記ステップ(3)で記憶していた乱数Ｒ２と前記復号文ＲＲＲ２を比較し、一致している場合には第１の暗号化ＩＣ８４及び第１の暗号化ＩＣ８４を含んだ第１の機器８１の正当性を認証する。

(9) 第１の暗号化ＩＣ８４において、前記乱数Ｒ１と前記分離データＲＲ２を結合することでデータ転送鍵Ｋを生成する。

【００８４】(10) 第２の暗号化ＩＣ８６において、前記復号文ＲＲ１と前記乱数Ｒ２を用いてデータ転送鍵Ｋを生成する。

(11) 第１の機器８１の第１の暗号化ＩＣ８４において、ＭＰＵ８３から送られてくるブロック化されたデジタル著作物ｍｊ（６４ビット）を上記ステップ(9)で得られたデータ転送鍵Ｋを用いて暗号化し、得られた暗号文Ｃｊを第２の機器８２に送信する処理を、転送すべき全てのデジタル著作物を送信し終えるまで繰り返す。

【００８５】(12) ステップ(11)に対応して、第２の機器８２の第２の暗号化ＩＣ８６において、第１の機器８１が送信した暗号化された上記デジタル著作物Ｃｊ（６４ビット）を受信し、上記ステップ(10)で得られたデータ転送鍵Ｋを用いて復号化し、得られたデジタル著作物ｍｍｊをＭＰＵ８５に送る。この復号化は上記デジタル著作物Ｃｊが第１の機器８１から送信されてくる限り繰り返す。

【００８６】このようにして、実施の形態３の暗号化装置により、実施の形態１及び２の場合と同様に、第１の機器７１と第２の機器７２間で相互認証とデータ転送鍵Ｋの共有化とデータの暗号通信とが行われる。なお、上記ステップ(1)(2)(6)(7)においては１つの乱数の暗号化、ステップ(3)(4)においては２つの乱数の結合の暗号化を行っている。６４ビット幅のＥ関数と逆変換アルゴリズムＤを用いる場合には、各乱数を３２ビットとして、前者については残りの３２ビットの入力に固定の３２ビットの値をパディングするとよい。例えば、乱数を下位３２ビットとし、上位３２ビットを固定的に全てゼロとする等である。また後者については結合した６４ビットをそのまま各関数に入力するとよい。

【００８７】また、各乱数のビット長を倍の６４ビットにする場合には、前者はそのまま関数に入力し、後者については各関数を２回繰り返して用い、例えばＣＢＣモードのように連鎖のある暗号を行えばよい。以上述べた実施の形態３においては、実施の形態１及び２とは異なり、認証のための乱数とデータ転送鍵の共有化のための乱数は兼用されている。そして、認証のための乱数生成や認証のための比較処理は暗号化ＩＣ内で行われている。従って、乱数はそのままでは暗号化ＩＣの外に現れないため、暗号化ＩＣを解読器として用いる攻撃に対して、より安全である。また、このことにより、各乱数のビット数が少なくても十分な安全性を確保することができる。

（実施の形態４）次に、実施の形態４に係る暗号化装置について説明する。

【００８８】本装置は、暗号化ＩＣのコンパクト化を追求した実施形態であり、一方向認証を採用している点、及び、データ転送鍵が公開される点において、上記実施の形態１～３と相違する。但し、暗号アルゴリズムＥ及びその逆変換アルゴリズムＤは秘密にされていることを前提とする。図５は、第１の機器９１から第２の機器９２にデジタル著作物ｍｊを転送する場合の処理シーケンスを示す図である。

【００８９】図６は、第１の暗号化ＩＣ９４のハードウェア構成を示すブロック図である。

(1) まず、第１の暗号化ＩＣ９４の乱数生成部１０１はチャレンジデータとデータ転送鍵を兼用する乱数Ｒ１を生成し、乱数格納部１０２に格納すると共に、外部Ｉ／Ｆ部１００を介して第２の機器９２に送信する。

(2) 第２の暗号化ＩＣ９６は、受信した乱数Ｒ１に対して、予め第１の暗号化ＩＣ９４と共通に所有している認証鍵Ｓを用いて復号化し、得られた復号文Ｃ１を第１の機器９１に送信する。

【００９０】(3) 第１の暗号化ＩＣ９４では、Ｅ関数１０６は、外部Ｉ／Ｆ部１００及びスイッチ１０５を介して受信した復号文Ｃ１に対して、認証鍵Ｓ格納部１０３に予め格納された上記認証鍵Ｓと同じものを用いて暗号化する。その結果得られたデータＲＲ１は、スイッチ１０７を経て比較部１０８に送られ、ここで、乱数格納部１０２に保持されていた乱数Ｒ１と比較される。

【００９１】(4) その結果一致している場合には、第２の機器９２は正当な機器であると認証できるので、比較部１０８は、乱数格納部１０２に保持されていた乱数Ｒ１がデータ転送鍵として用いられるように、スイッチ１０４を制御する。

(5) Ｅ関数１０６は、ＭＰＵ９３から外部Ｉ／Ｆ部１００及びスイッチ１０５を経て送られてくるデジタル著作物ｍｊに対して、スイッチ１０４を経て送られてくる乱数Ｒ１を用いて暗号化し、スイッチ１０７及び外部Ｉ／Ｆ部１００を介して第２の機器９２に送信する。

【００９２】(6) 第２の機器９２の第２の暗号化ＩＣ９６においては、第１の機器９１から送られてきたデジタル著作物Ｃｊに対して、上記ステップ(2)で受信した乱

数Ｒ１をデータ転送鍵として用いて復号化し、得られたデジタル著作物ｍｍｊをＭＰＵ９５に送る。このようにして、本実施の形態では、実施の形態１～３の場合よりも少ないステップと構成要素により、認証とデータ転送鍵の共有化と暗号通信とが実現される。

【００９３】なお、本実施の形態では、第１の機器９１から第２の機器９２に送信された乱数Ｒ１がそのままデータ転送鍵として用いられているために、データ転送鍵は容易に第３者に知られ得る。ところが、そのデータ転送鍵を知った第３者がデジタル著作物Ｃｊを盗聴し復号化しようとしても、上述したように暗号アルゴリズムＥ及びその逆変換アルゴリズムＤは秘密にされているので、その試みは成功しない。

【００９４】また、その第３者が都合のよい乱数Ｒ１を偽造することで暗号アルゴリズムを解読しようとしても、新たな乱数Ｒ１を乱数格納部１０２に格納できるのは乱数生成部１０１だけであり、この第１の暗号化ＩＣ９４の外部から新たな乱数Ｒ１を乱数生成部１０１に格納する手段は存在しないので、その試みも成功しない。このように、暗号アルゴリズム及びその逆変換アルゴリズムが秘密にされるならば、本実施の形態のようなコンパクトな暗号化ＩＣによっても認証とデータ転送鍵の生成と暗号通信を実現することができる。

【００９５】なお、上記実施の形態１～４において、認証鍵Ｓを暗号化ＩＣに設定する（記憶させる）方法としては以下が好ましい。つまり、認証鍵Ｓの一部は暗号化ＩＣの製造時に予め設定しておき、残る部分はその暗号化ＩＣの製造後に書き込む方法である。具体的には、認証鍵Ｓ格納部６４の一部は、認証鍵Ｓの一部を予め書き込んだマスクＲＯＭで構成し、残る部分は、プログラマブルに書き込み可能な追記ＲＯＭで構成する。

【００９６】これは、マスクＲＯＭのみで構成した場合には、最終的な暗号化ＩＣの作成のために人手を介さないために安全である反面、リバースエンジニアリングによるチップ解析で設定値の解析が容易であるという欠点があり、一方、追記ＲＯＭのみで構成した場合には、設定値のリバースエンジニアリングによる解析が困難である反面、設定に人手を介するためミスが混入したり不正が可能となるという欠点があるので、それら両方の欠点を補うためである。

【００９７】また、上記実施の形態１～４の暗号通信における暗号アルゴリズムの具体例として、次のようなものであってもよい。送信側でデジタル著作物を６４ビットのブロックに分割し、前記データ転送鍵Ｋ（６４ビット）とビットごとの排他的論理和をとる。その結果を暗号文とする。受信側でも同様に、受信した６４ビットの暗号文とデータ転送鍵Ｋとの排他的論理和をとればよい。これによって、もとのブロックに復号される。

【００９８】また、データ転送鍵Ｋを固定とするのではなく、それらブロックごとに、用いられるデータ転送鍵

Ｋを送信側と受信側で同期をとりながら更新していく方法もある。その更新のために、前記Ｅ関数や逆変換アルゴリズムＤを用いてもよい。ブロック内の暗号／復号は先に述べた排他的論理和であってもよい。また、上記実施の形態１～４において、認証方法としてチャレンジレスポンス型のいくつかの例が示されているが、本発明はこれらの例に限られない。例えば、認証側の暗号化ＩＣで乱数を生成し、これをチャレンジデータとして送付し、証明側から返送されたレスポンスデータと認証側で生成した参照用のレスポンスデータとを比較する、というチャレンジレスポンス型の別の例であってもよい。

【００９９】なお、上記実施の形態１～４において、小さな回路規模で認証と暗号通信を安全に行なう技術を開示したが、安全性の強度とそのために必要な回路規模とはトレードオフの関係にあることは言うまでもない。従って、もしＭＰＵや暗号化ＩＣ内に実装できる回路規模に余裕がある場合には、以下の目的のために、データ変換Ｆ（）を実行する新たな変換手段を追加導入することで、暗号通信の安全性を強化することができる。

（１）その一つは、平文のチャレンジデータや平文のレスポンスデータが伝送路を流れないようにすることである。

【０１００】例えば、図１に示された第１の機器５１が第２の機器５２を認証する処理シーケンス（ステップ(1)(3)(6)(7)）において、以下のように変更する。ステップ(6)において、第２の暗号化ＩＣ５６は、分離データＲＲ１をＭＰＵ５３に送るのではなく、その分離データＲＲ１に所定の変換Ｆ（）を施し、その結果得られたデータＦ（ＲＲ１）をＭＰＵ５３に送る。

【０１０１】ステップ(7)において、ＭＰＵ５３は、乱数Ｒ１と分離データＲＲ１とを比較するのではなく、乱数Ｒ１に上記ステップ(6)で用いたものと同じ変換Ｆ（）を施し、その結果得られたデータＦ（Ｒ１）と第２の暗号化ＩＣ５６から送られてきたデータＦ（ＲＲ１）とを比較する。このようにすることで、暗号文Ｃ１とその平文の一部ＲＲ１とが伝送路を流れることが回避されるので、既知平文攻撃に対する安全性が強化される。

（２）もう一つは、チャレンジデータをそのままデータ転送鍵として用いないようにすることである。

【０１０２】例えば、図５に示されたステップ(5)において、第１の暗号化ＩＣ９４は、乱数Ｒ１をそのままデータ転送鍵として用いるのではなく、乱数Ｒ１に所定の変換Ｆ（）を施し、その結果得られたデータＦ（Ｒ１）をデータ転送鍵として用いる。同様に、ステップ(6)において、第２の暗号化ＩＣ９６は、乱数Ｒ１をそのままデータ転送鍵として用いるのではなく、乱数Ｒ１に上記ステップ(5)で用いたものと同じ変換Ｆ（）を施し、その結果得られたデータＦ（Ｒ１）をデータ転送鍵として用いる。

【０１０３】このようにすることで、データ転送鍵Ｆ（Ｒ１）を秘匿することができ、暗号通信の安全性が強化される。

（３）さらにもう一つは、結合処理を複雑にすることである。例えば、図１に示されたステップ(9)において、第１の暗号化ＩＣ５４は、乱数Ｒ３と分離データＲＲ４とを単に桁方向に結合するのではなく、これらＲ３、ＲＲ４に所定の変換Ｆ（）を施し、その結果得られたデータＦ（Ｒ３，ＲＲ４）をデータ転送鍵Ｋとする。

【０１０４】同様に、ステップ(10)において、第２の暗号化ＩＣ５６は、乱数Ｒ４と分離データＲＲ３とを単に桁方向に結合するのではなく、これらＲ４、ＲＲ３に上記ステップ(9)で用いたものと同じ変換Ｆ（）を施し、その結果得られたデータＦ（Ｒ３，ＲＲ４）をデータ転送鍵Ｋとする。このようにすることで、データ転送鍵Ｋの生成手順が複雑化され、暗号通信の安全性が強化される。

（具体的な通信システムへの適応例）以上のように、本発明に係る暗号化装置は、規模の小さな暗号化ＩＣを備え、機器間通信の安全性を確保するための必要最小限の機能を持っている。従って、本暗号化装置は、秘密通信が必要とされ、かつ、小型であることが要求される通信機器、例えば、携帯電話機やデジタル著作物を扱うマルチメディア関連機器等に好適な装置である。

【０１０５】図７は、本発明に係る暗号化装置の具体的な通信システムへの適用例を示す図であり、映画等のデジタル著作物の再生システムの概観を示す。このシステムは、上記実施形態における第１の機器に対応する光ディスクドライブ装置１１０と第２の機器に対応する映像再生装置１１１とそれらを接続するＳＣＳＩケーブル１１６等からなる。光ディスクドライブ装置１１０で読み出した圧縮映像データを暗号化して映像再生装置１１１に転送し、そこで映像再生するシステムである。

【０１０６】図８は、光ディスクドライブ装置１１０の構成を示すブロック図である。光ディスクドライブ装置１１０は、装置全体の制御を行うＭＰＵ１２４と、映像再生装置１１１との通信インタフェースであるＳＣＳＩコントローラ１２１と、光ヘッド１２５を制御して光ディスク１１５から映像データを読み出し制御する読み出し制御部１２２と、上述の実施形態１～４における第１の機器の暗号化ＩＣに相当する暗号化ＩＣ１２３とからなり、映像再生装置１１１が正当な機器であることを認証した後に、光ディスク１１５に記録された映像データを読み出して暗号化ＩＣ１２３において暗号化し、ＳＣＳＩケーブル１１６を介して映像再生装置１１１に転送する。

【０１０７】図９は、光ディスクドライブ装置１１０の内部に実装される回路基板の概観を示す図である。暗号化ＩＣ１２３は、１個のシリコン基板に形成されたＬＳＩであり、プラスチックでモールドされたフラットパッケージの形状をしている。図１０は、映像再生装置１１１の構成を示すブロック図である。映像再生装置１１１は、装置全体の制御を行うＭＰＵ１３１と、光ディスクドライブ装置１１０との通信インタフェースであるＳＣＳＩコントローラ１３０と、上述の実施形態１～４の第２の機器の暗号化ＩＣに相当する暗号化ＩＣ１３２と、暗号化ＩＣ１３２で復号された圧縮映像データの伸長を行うＭＰＥＧデコーダ１３３と、伸長された映像データをアナログ映像信号に変換してＣＲＴ１１２及びスピーカ１１４に映像出力するＡＶ信号処理部１３４とから構成される。

【０１０８】本発明に係る暗号化装置をこのような映像再生システムに適用することで、光ディスク１１５に記録されたデジタル著作物は不正コピー等から保護され、マルチメディア関連製品の流通市場における健全な発展が期待できる。

【０１０９】

【発明の効果】以上の説明から明らかなように、本発明に係る暗号化装置は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、前記データ転送鍵の共有化のための第１乱数を生成する第１乱数生成手段と、前記第１乱数生成手段により生成された第１乱数を保持する第１乱数保持手段と、前記第１乱数生成手段により生成された第１乱数を前記暗号通信の相手機器に送信する第１送信手段と、前記第１乱数保持手段に保持された第１乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、前記第１乱数生成手段、前記第１乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、１個のＩＣ内の回路で実現され、前記第１乱数保持手段は、前記ＩＣの外部からアクセスできない領域に前記第１乱数を保持することを特徴とする。

【０１１０】これにより、データ転送鍵の生成に直接関連する第１乱数は外部からアクセスできない暗号化ＩＣの内部に保持されるので、時変のデータ転送鍵は各機器に安全に共有され、暗号通信が行われる。また、暗号化ＩＣは、機器間通信の安全性を確保するための必要最小限の機能を持つので、小さな回路で実現することができる。

【０１１１】ここで、前記暗号化装置はさらに、前記第１乱数生成手段により生成された第１乱数を暗号化する第１暗号化手段を備え、前記第１暗号化手段は、前記ＩＣ内の回路で実現され、前記第１送信手段は、前記第１暗号化手段で暗号化された第１乱数を前記相手機器に送信するとすることもできる。これにより、第３者はデータ転送鍵の生成に直接関連する第１乱数を知ることができなくなるので、データ転送鍵の秘密性が維持され、たとえ暗号アルゴリズム及びその逆変換アルゴリズムが知

られたとしても暗号通信は維持される。

【０１１２】ここで、前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記相手機器に送信するチャレンジデータ用の第２乱数を生成する第２乱数生成手段と、前記チャレンジデータに対して前記相手機器から返信されてきたレスポンスデータと前記第２乱数とが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段とを備え、前記データ転送鍵生成手段は、前記認証がなされた場合に前記データ転送鍵を生成するとすることもできる。

【０１１３】これにより、機器間の相互認証が成功したときに同時に正規のデータ転送鍵が生成されることになり、秘密通信の安全性が向上される。ここで、前記第２乱数生成手段及び前記認証手段は、前記ＩＣ外の回路で実現されているとすることもできる。これにより、通信システムの安全性に関連しない部分、即ち、データ転送鍵の生成に直接関連しない処理部は暗号化ＩＣの外に設けられるので、暗号化ＩＣの規模が不要に大きくなることが抑制される。

【０１１４】ここで、前記暗号化装置はさらに、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第１分離データと残る第２分離データとに分離する分離手段と、前記第１分離データを前記相手機器に返信する第２送信手段とを備え、前記第１暗号化手段は、前記第１乱数と前記第２乱数とを結合し、その結果得られた結合データを暗号化し、前記データ転送鍵生成手段は、前記第１乱数と前記第２分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段及び前記分離手段は、前記ＩＣ内の回路で実現されているとすることもできる。

【０１１５】また、前記暗号化装置はさらに、前記第２乱数をチャレンジデータとして前記相手機器に送信する第２送信手段と、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第１分離データと残る第２分離データとに分離する分離手段とを備え、前記認証手段は、前記第１分離データを前記相手機器から返信されてきたレスポンスデータとして前記判断及び認証をし、前記第１暗号化手段は、前記相手機器から送信されてきたチャレンジデータと前記第１乱数とを結合し、その結果得られた結合データを暗号化し、前記データ転送鍵生成手段は、前記第１乱数と前記第２分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段及び前記分離手段は、前記ＩＣ内の回路で実現されているとすることもできる。

【０１１６】これにより、機器間通信の安全性を確保するための必要最小限の機能を持ち、規模の小さな暗号化ＩＣを備えた暗号化装置が実現される。ここで、前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第１暗号化手段及び前記復号化手段の少なくとも１つのものと同一であることを特徴とするとすることもできる。

【０１１７】これにより、転送データ暗号化手段と第１暗号化手段や復号化手段を１個の変換器で兼用して実装することが可能となるので、暗号化ＩＣの回路規模が削減される。ここで、前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第１暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であるとすることもできる。

【０１１８】これにより、転送データのサイズが大きいために何度もその暗号化を繰り返すような場合であっても、暗号化のためにデータ転送時間が大幅に長くなってしまうという不具合が回避される。ここで、前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化するとすることもできる。

【０１１９】これにより、データサイズの大きい転送データの暗号通信に対しても、本暗号化装置を適用することが可能となる。ここで、前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうとすることもできる。

【０１２０】これにより、簡易な論理回路で転送データ暗号化手段を実現することが可能となる。ここで、前記第１暗号化手段での暗号と前記復号化手段での復号化とは、同一の変換アルゴリズムであるとすることもできる。これにより、第１暗号化手段と復号化手段を１個の変換器で兼用して実装することが可能となり、暗号化ＩＣの回路規模が削減される。

【０１２１】ここで、前記第１暗号化手段及び前記復号化手段は、予め前記ＩＣ内に保持された鍵データを用いて前記暗号化及び復号化を行い、その鍵データの一部は、前記ＩＣ内のマスクＲＯＭ領域に格納され、残る一部は、前記ＩＣ内の追記ＲＯＭ領域に格納されているとすることもできる。これにより、認証鍵をマスクＲＯＭのみで構成した場合における欠点と、追記ＲＯＭのみで構成した場合における欠点と補うことが可能となる。

【０１２２】ここで、前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記チャレンジデータに対して前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第１分離データと残る第２分離データとに分離する分離手段と、前記第１乱数と前記第１分離データとが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証

する認証手段と、前記認証がなされた場合に前記第２分離データを暗号化する第２暗号化手段と、暗号化された前記第２分離データをレスポンスデータとして前記相手機器に返信する第２送信手段とを備え、前記データ転送鍵生成手段は、前記第１乱数と前記第２分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段、前記分離手段及び前記第２暗号化手段は、前記ＩＣ内の回路で実現されているとすることもできる。

【０１２３】これにより、乱数を一つだけ生成し、それを認証用とデータ転送鍵の生成用の両方の目的に使用しているので、暗号化装置での乱数生成のための回路規模が軽減される。また、暗号化ＩＣの内部において認証のための乱数生成と比較処理を行っているので、暗号通信の安全性が高められる。

【０１２４】また、本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機が、それぞれ上記構成を備えるとすることもできる。これにより、送信機及び受信機間で相互認証が行われると共にデータ転送鍵が生成されること、データ転送鍵の生成に直接関連する乱数はそのままでは送受信されないこと、及び、データ転送鍵の生成に直接関連する２つの乱数はそれぞれ送信機及び受信機から提供されたものであることから、規模の小さな暗号化ＩＣを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムが実現される。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図２】図１に示された第１の暗号化ＩＣ５４のハードウェア構成を示すブロック図である。

【図３】本発明の第２の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図４】本発明の第３の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図５】本発明の第４の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図６】図５に示された第１の暗号化ＩＣ９４のハードウェア構成を示すブロック図である。

【図７】本発明に係る暗号化装置の具体的な通信システムへの適用例を示す図である。

【図８】図７に示された光ディスクドライブ装置１１０の構成を示すブロック図である。

【図９】同光ディスクドライブ装置１１０の内部に実装される回路基板の概観を示す図である。

【図１０】図７に示された映像再生装置１１１の構成を示すブロック図である。

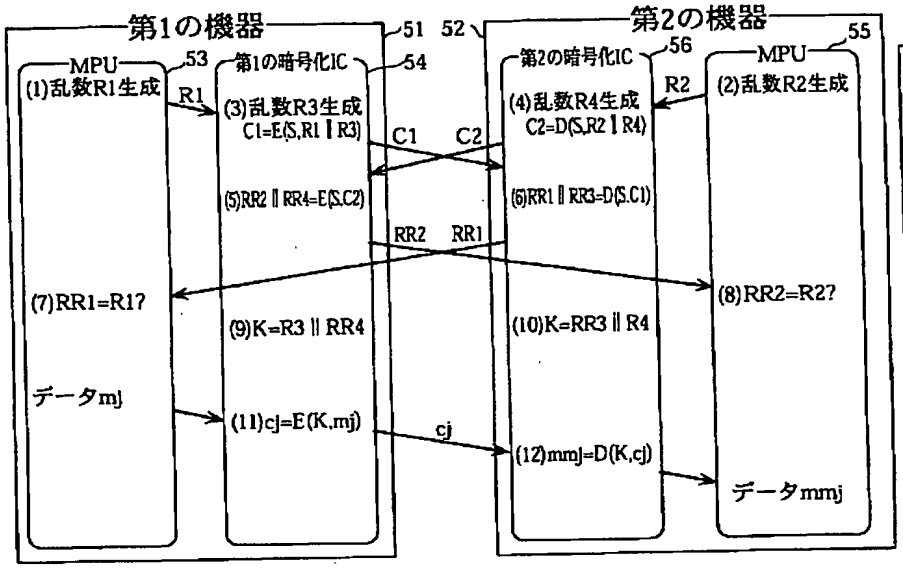
【図１１】第１の従来技術に係る一方向認証の処理シーケンスを示す図である。

【図１２】第２の従来技術に係る双方向認証の処理シーケンスを示す図である。

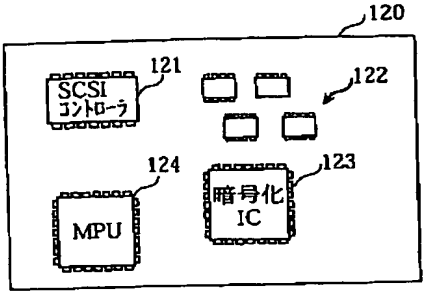
【符号の説明】

５１、７１、８１、９１　第１の機器
５２、７２、８２、９２　第２の機器
５３、７３、８３、９３　第１の機器のＭＰＵ
５４、７４、８４、９４　第１の暗号化ＩＣ
５５、７５、８５、９５　第２の機器のＭＰＵ
５６、７６、８６、９６　第２の暗号化ＩＣ
５９　データ転送鍵Ｋ生成部
６０、１０１　乱数生成部
６１、１００　外部Ｉ／Ｆ部
６２、１０２　乱数格納部
６３　結合部
６４、１０３　認証鍵Ｓ格納部
６５、６６、６８、１０４、１０５、１０７　スイッチ
６７、１０６　Ｅ関数
６９　分離部
７０　データ転送鍵Ｋ格納部
１０８　比較部
１１０　光ディスクドライブ装置
１１１　映像再生装置
１２１　ＳＣＳＩコントローラ
１２２　制御部
１２３　暗号化ＩＣ
１２４　ＭＰＵ
１２５　光ヘッド
１３０　ＳＣＳＩコントローラ
１３１　ＭＰＵ
１３２　暗号化ＩＣ
１３３　ＭＰＥＧデコーダ
１３４　ＡＶ信号処理部

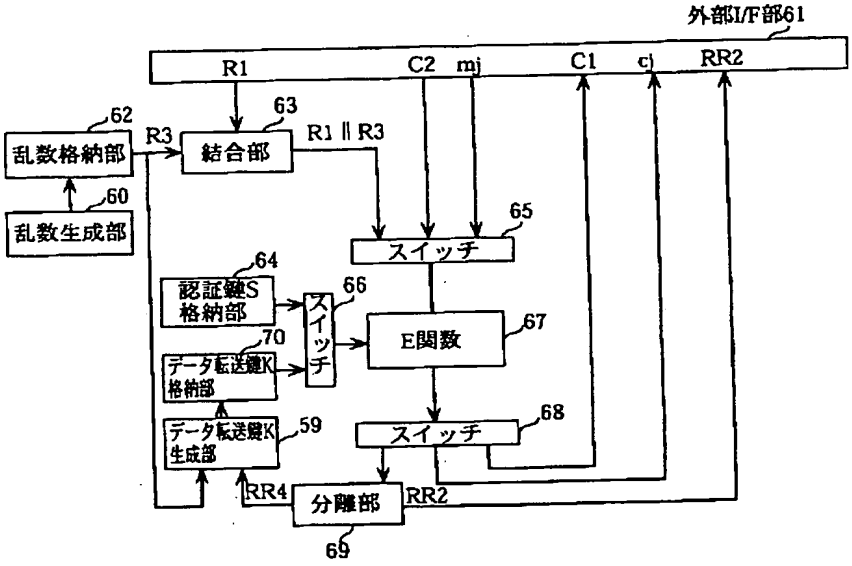
【図１】


第1の機器
第2の機器
MPU
(1)乱数R1生成
R1
53
第1の暗号化IC
54
(3)乱数R3生成
C1=E(S,R1 ‖ R3)
C1
C2
51
52
第2の暗号化IC
56
MPU
55
(4)乱数R4生成
C2=D(S,R2 ‖ R4)
R2
(2)乱数R2生成
(5)RR2 ‖ RR4=E(S,C2)
(6)RR1 ‖ RR3=D(S,C1)
RR2
RR1
(7)RR1=R1?
(8)RR2=R2?
(9)K=R3 ‖ RR4
(10)K=RR3 ‖ R4
データmj
(11)cj=E(K,mj)
cj
(12)mmj=D(K,cj)
データmmj

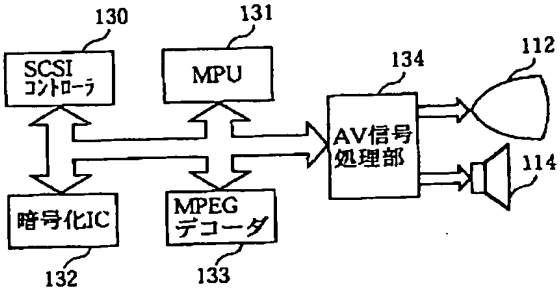
【図９】


120
SCSI
コントローラ
121
122
124
MPU
暗号化
IC
123

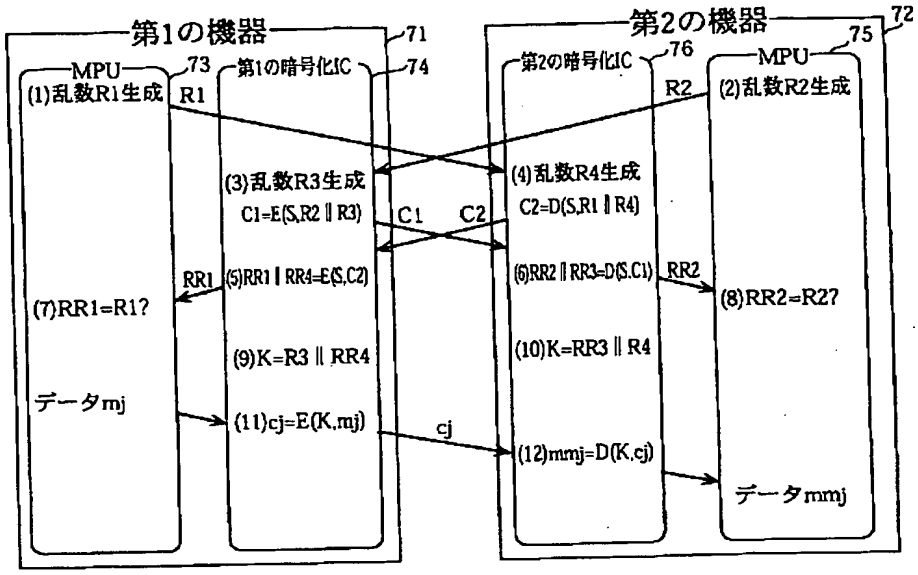
【図２】


外部I/F部61
R1
C2
mj
C1
cj
RR2
62
乱数格納部
R3
63
結合部
R1 ‖ R3
60
乱数生成部
65
スイッチ
64
認証鍵S
格納部
66
スイッチ
67
E関数
70
データ転送鍵K
格納部
データ転送鍵K
生成部
59
68
スイッチ
RR4
分離部
RR2
69

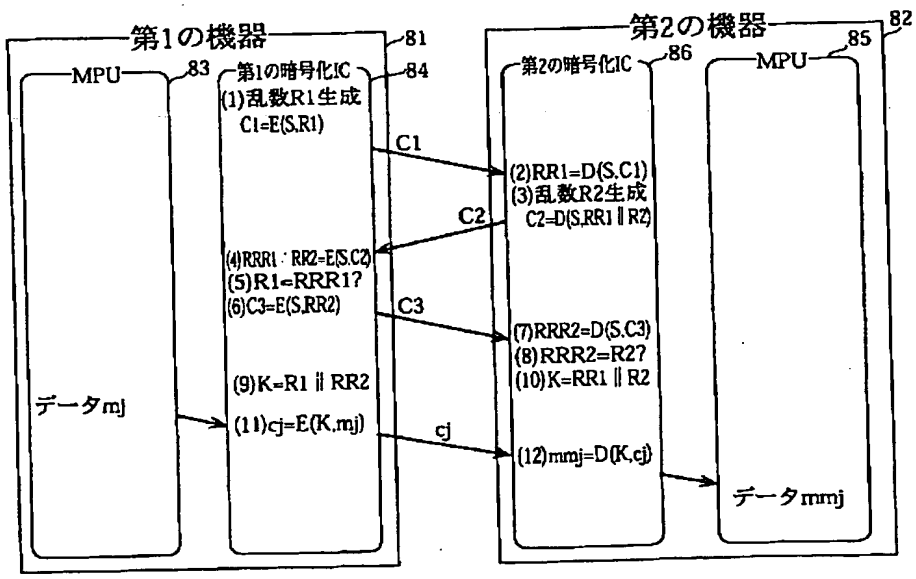
【図１０】


130
SCSI
コントローラ
131
MPU
134
112
AV信号
処理部
114
暗号化IC
MPEG
デコーダ
132
133

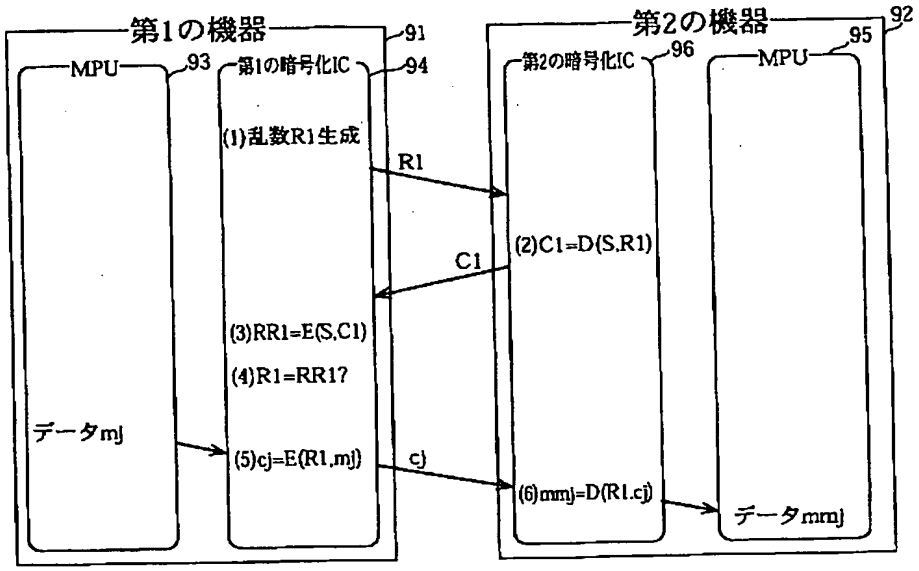
【図３】


第1の機器
71
MPU
73
(1)乱数R1生成
R1
第1の暗号化IC
74
(3)乱数R3生成
C1=E(S,R2 ‖ R3)
C1
C2
RR1
(5)RR1 ‖ RR4=E(S,C2)
(7)RR1=R1?
(9)K=R3 ‖ RR4
データmj
(11)cj=E(K,mj)
cj
第2の機器
72
第2の暗号化IC
76
(4)乱数R4生成
C2=D(S,R1 ‖ R4)
(6)RR2 ‖ RR3=D(S,C1)
(10)K=RR3 ‖ R4
(12)mmj=D(K,cj)
MPU
75
R2
(2)乱数R2生成
RR2
(8)RR2=R2?
データmmj

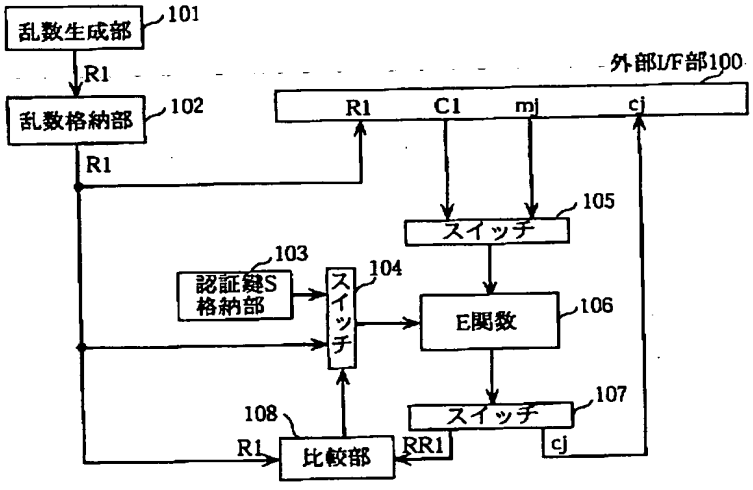
【図４】


第1の機器
81
MPU
83
第1の暗号化IC
84
(1)乱数R1生成
C1=E(S,R1)
C1
C2
(4)RRR1 ‖ RR2=E(S,C2)
(5)R1=RRR1?
(6)C3=E(S,RR2)
C3
(9)K=R1 ‖ RR2
データmj
(11)cj=E(K,mj)
cj
第2の機器
82
第2の暗号化IC
86
(2)RR1=D(S,C1)
(3)乱数R2生成
C2=D(S,RR1 ‖ R2)
(7)RRR2=D(S,C3)
(8)RRR2=R2?
(10)K=RR1 ‖ R2
(12)mmj=D(K,cj)
MPU
85
データmmj

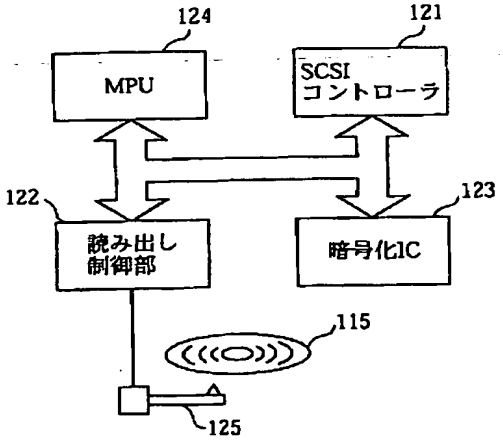
【図５】


第1の機器
91
MPU
93
第1の暗号化IC
94
(1)乱数R1生成
R1
C1
(2)C1=D(S,R1)
(3)RR1=E(S,C1)
(4)R1=RR1?
データmj
(5)cj=E(R1,mj)
cj
(6)mmj=D(R1,cj)
データmmj
第2の機器
92
第2の暗号化IC
96
MPU
95

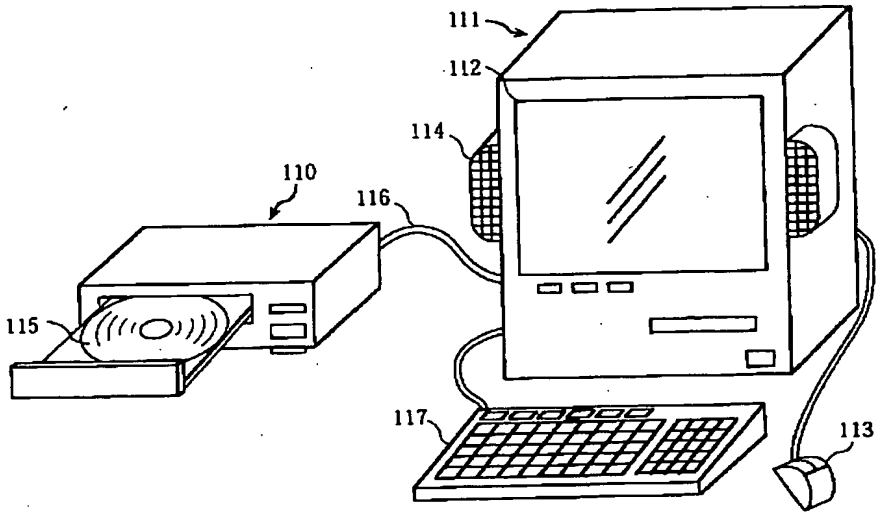
【図６】


乱数生成部
101
R1
乱数格納部
102
外部I/F部100
R1
C1
mj
cj
スイッチ
105
認証鍵S格納部
103
スイッチ
104
E関数
106
スイッチ
107
108
R1
比較部
RR1
cj

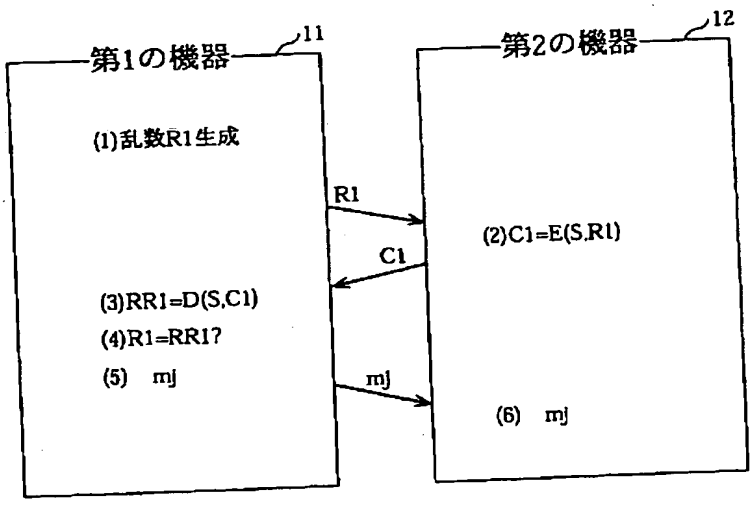
【図８】


124
121
MPU
SCSIコントローラ
122
123
読み出し制御部
暗号化IC
115
125

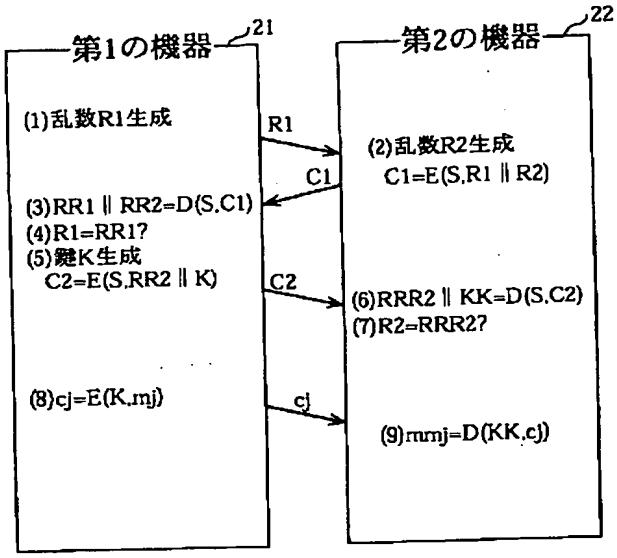
【図７】


111
112
114
110
116
115
117
113

【図１１】


第1の機器
11
(1)乱数R1生成
R1
C1
(3)RR1=D(S,C1)
(4)R1=RR1?
(5) mj
mj
第2の機器
12
(2)C1=E(S,R1)
(6) mj

【図１２】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	F I		技術表示箇所
			H０４L　9/00	６７５Ａ	